Random numbers certified by Bell's theorem

S. Pironio[1,2]*, A. Acín[3,4]*, S. Massar[1]*, A. Boyer de la Giroday[5], D. N. Matsukevich[6], P. Maunz[6], S. Olmschenk[6], D. Hayes[6], L. Luo[6], T. A. Manning[6] & C. Monroe[6]

Randomness is a fundamental feature of nature and a valuable resource for applications ranging from cryptography and gambling to numerical simulation of physical and biological systems. Random numbers, however, are difficult to characterize mathematically[1], and their generation must rely on an unpredictable physical process[2–6]. Inaccuracies in the theoretical modelling of such processes or failures of the devices, possibly due to adversarial attacks, limit the reliability of random number generators in ways that are difficult to control and detect. Here, inspired by earlier work on non-locality-based[7–9] and device-independent[10–14] quantum information processing, we show that the non-local correlations of entangled quantum particles can be used to certify the presence of genuine randomness. It is thereby possible to design a cryptographically secure random number generator that does not require any assumption about the internal working of the device. Such a strong form of randomness generation is impossible classically and possible in quantum systems only if certified by a Bell inequality violation[15]. We carry out a proof-of-concept demonstration of this proposal in a system of two entangled atoms separated by approximately one metre. The observed Bell inequality violation, featuring near perfect detection efficiency, guarantees that 42 new random numbers are generated with 99 per cent confidence. Our results lay the groundwork for future device-independent quantum information experiments and for addressing fundamental issues raised by the intrinsic randomness of quantum theory.

The characterization of true randomness is elusive. There exist statistical tests used to verify the absence of certain patterns in a stream of numbers[16,17], but no finite set of tests can ever be considered complete, as there may be patterns not covered by such tests. For example, certain pseudo-random number generators are deterministic in nature, yet produce results that satisfy all the randomness tests[18]. At a more fundamental level, there is no such thing as true randomness in the classical world: any classical system admits in principle a deterministic description and thus appears random to us as a consequence of a lack of knowledge about its fundamental description. Quantum theory is, on the other hand, fundamentally random; yet, in any real experiment the intrinsic randomness of quantum systems is necessarily mixed-up with an apparent randomness that results from noise or lack of control of the experiment. It is therefore unclear how to certify or quantify unequivocally the observed random behaviour even of a quantum process.

These considerations are of direct relevance to applications of randomness, and in particular cryptographic applications. Imperfections in random number generators[2–6,18] (RNGs) can introduce patterns undetected by statistical tests but known to an adversary. Furthermore, if the device is not trusted but viewed as a black box prepared by an adversary, no existing RNGs can establish the presence of private randomness. Indeed, one can never exclude the possibility that the numbers were generated in advance by the adversary and copied into a memory located inside the device.

Here we establish a fundamental link between the violation of Bell inequalities and the unpredictable character of the outcomes of quantum measurements and show, as originally proposed in ref. 14, that the non-local correlations of quantum states can be used to generate certified private randomness. The violation of a Bell inequality[15] guarantees that the observed outputs are not predetermined and that they arise from entangled quantum systems that possess intrinsic randomness. For simplicity, we consider the Clauser–Horn–Shimony–Holt (CHSH) form of Bell inequality[19], but our approach is general and applies to any Bell inequality. We thus consider two separate systems that can each be measured in two different ways, with a measurement on each system resulting in one of two values (Fig. 1). The binary variables x and y describe the type of measurement performed on each system, resulting in respective binary measurement outcomes a and b. We quantify the Bell inequality violation through the CHSH correlation function[19]

$$I=\sum_{x,y}(-1)^{xy}[P(a=b|xy)-P(a\neq b|xy)] \tag{1}$$

where $P(a=b|xy)$ is the probability that $a=b$ when settings (x, y) are chosen, and $P(a\neq b|xy)$ is defined analogously. Systems that admit a local, hence deterministic[20], description satisfy $I\leq 2$. Certain measurements performed on entangled states, however, can violate this inequality.

In order to estimate the Bell violation, the experiment is repeated n times in succession. The measurement choices (x, y) for each trial are generated by an identical and independent probability distribution $P(xy)$. We denote the final output string after the n runs $r=(a_1, b_1; \dots; a_n, b_n)$ and the input string $s=(x_1, y_1; \dots; x_n, y_n)$. An estimator $\hat{I}$ of the CHSH expression, equation (1), determined from the observed data is given by

$$\hat{I}=\frac{1}{n}\sum_{x,y}(-1)^{xy}[N(a=b,xy)-N(a\neq b,xy)]/P(xy) \tag{2}$$

where $N(a=b, xy)$ is the number of times that the measurements x, y were performed and that the outcomes a and b were found equal after n realizations, and where $N(a\neq b, xy)$ is defined analogously.

The randomness of the output string r can be quantified by the min-entropy[21] $H_\infty(R|S)=-\log_2[\max_r P(r|s)]$, where $P(r|s)$ is the conditional probability of obtaining the outcomes r when the measurements s are made and the maximum is taken over all possible values of the output string r. We show (Supplementary Information A) that the min-entropy of the outputs r is bounded by

$$H_\infty(R|S)\geq nf\left(\hat{I}-\varepsilon\right) \tag{3}$$

[1] Laboratoire d'Information Quantique, CP 225, Université Libre de Bruxelles, Bvd Du Triomphe, 1050 Bruxelles, Belgium. [2] Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland. [3] ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain. [4] ICREA-Institucio Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain. [5] Cavendish Laboratory, Cambridge University, Cambridge CB3 0HE, UK. [6] Joint Quantum Institute, University of Maryland Department of Physics and National Institute of Standards and Technology, College Park, Maryland 20742, USA.
*These authors contributed equally to this work.

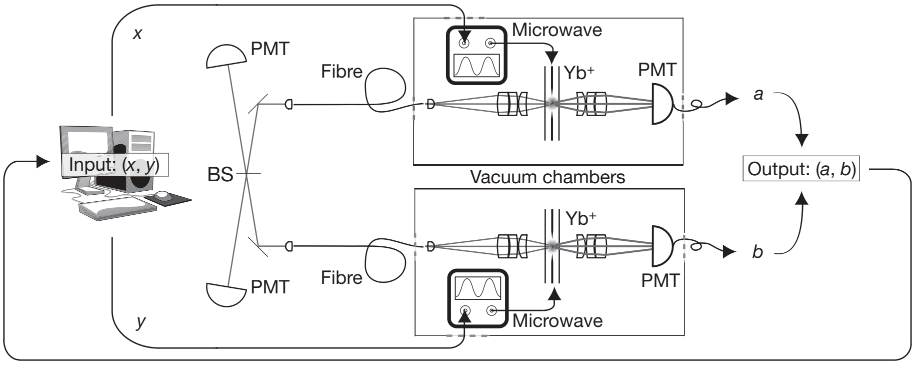

Figure 1 | Experimental realization of private random number generator using two ^{171}Yb^{+} qubits trapped in independent vacuum chambers. Each atom emits a single photon (to the left) that is entangled with its host atomic qubit and coupled into optical fibres; the interference of the photons on the beamsplitter (BS) and subsequent coincidence detection on photomultiplier tubes (PMT) herald the entanglement of the atomic qubits[26]. After the qubits are entangled, binary random inputs (x, y) are fed to microwave oscillators that coherently rotate each qubit in one of two ways before measurement[26]. Each qubit is finally measured through fluorescence that is collected by the PMTs[25] (right), resulting in the binary outputs (a, b). Abstractly, we can view this scheme as composed of two black boxes that receive inputs x, y and produce outputs a, b. In our theoretical analysis, no hypotheses are made about the internal working of the devices, but the classical and quantum information flowing in and out of the boxes is restricted (dashed lines). In particular, the two boxes are free to communicate before inputs are introduced (to establish shared entanglement), but are no longer allowed to interact during the measurement process. Moreover, the values of the inputs are revealed to the boxes only at the beginning of the measurement process. In the experiment, no active measures are taken to control the flow of information in and out of the systems. However, once the atoms are entangled, direct interaction between them is negligible. In addition, the value of the chosen measurement bases (x, y), obtained by combining the outputs of several random number generators, is unlikely to be correlated to the state of the atoms before the measurement microwave pulses are applied. The conditions for the bound (equation (3)) on the entropy of the outputs should thus be satisfied.

with probability greater than $1-\delta$, where $\varepsilon = O\left(\sqrt{-\log\delta/(q^2 n)}\right)$ is a statistical parameter and $q = \min_{x,y} P(xy)$ is the probability of the least probable input pair. The function $f(I)$ is obtained using semidefinite programming[22,23] and presented in Fig. 2. To derive the bound given as equation (3), we make the following assumptions: (1) the two observed systems satisfy the laws of quantum theory; (2) they are separated and non-interacting during each measurement step i; and (3) the inputs x_i, y_i are generated by random processes that are independent and uncorrelated from the systems and their value is revealed to the systems only at step i (Fig. 1). Other than these assumptions, no constraints are imposed on the states, measurements, or the dimension of the Hilbert space. We do not even assume that the system behaves identically and independently for each trial; for instance, the devices may have an internal memory (possibly quantum), so that the ith measurement can depend on the previous $i-1$ results and measurement settings. Any value of the min-entropy smaller than that given by equation (3) is incompatible with quantum theory. The observed CHSH quantity $\hat{I}$ thus provides a bound (Fig. 3) on the randomness produced by the quantum devices, independent of any apparent randomness that could arise from noise or limited control over the experiment.

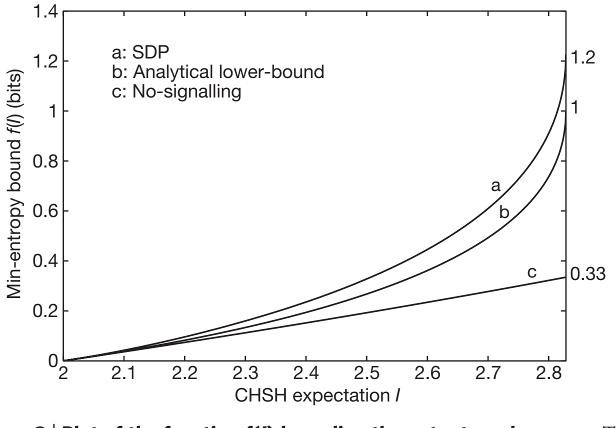

Figure 2 | Plot of the function *f(I)* bounding the output randomness. The function $f(I)$ can be interpreted as a bound on the min-entropy per use of the system for a given CHSH expectation I, in the asymptotic limit of large n where finite statistics effects (the parameter ε in equation (3)) can be neglected. The function $f(I)$ (curve a) is derived through semidefinite programming using the techniques of refs 22 and 23 (semidefinite programming is a numerical method that is guaranteed to converge to the exact result). Curve b corresponds to the analytical lower-bound $f(I) \geq -\log_2\left[1-\log_2\left(1+\sqrt{2-\frac{I^2}{4}}\right)\right]$. Curve c corresponds to the minimal value $f(I) = -\log_2(3/2 - I/4)$ of the min-entropy implied by the no-signalling principle alone. The function $f(I)$ starts at zero at the local threshold value $I = 2$. Systems that violate the CHSH inequality ($I > 2$), on the other hand, satisfy $f(I) > 0$, that is, have a positive min-entropy.

This result can be exploited to construct a novel RNG where the violation of a Bell inequality guarantees that the output is random and private from any adversary, even in a device-independent scenario[12,13] where the internal workings of the two quantum devices are unknown or not trusted (Supplementary Information B). Some amount of randomness at the inputs is necessary to perform the statistical tests used to estimate the Bell inequality violation. Hence what we describe here is a randomness expansion scheme[14], where a small private random seed is expanded into a longer private random string. The randomness used to choose the inputs needs not be divulged and can be used subsequently for another task. The final random string, the concatenation of the input and output random strings, is thus manifestly longer than the initial one. However, when n becomes sufficiently large, a catalysis effect is possible wherein a seed string of length $O\left(\sqrt{n}\log\sqrt{n}\right)$ produces a much longer random output string of entropy $O(n)$, as illustrated in Fig. 3 (Supplementary Information B). This is possible because I can be adequately estimated without consuming much randomness by using the same input pair most of the time (for example, $(x, y) = (0, 0)$) while only seldom sampling from the other possibilities, in which case $q \ll 1$. This follows from the fact that the CHSH expression depends only the conditional probabilities $P(ab|xy)$, which can be estimated even if x, y are not uniformly distributed.

Although the final output string may not be uniformly random (it may not even pass one of the usual statistical tests[16,17] of randomness), we are guaranteed that its entropy is bounded by equation (3). With the help of a small private random seed, the output string can then be classically processed using a randomness extractor[24] to convert it into a string of size $nf\left(\hat{I}-\varepsilon\right)$ that is nearly uniform and uncorrelated to

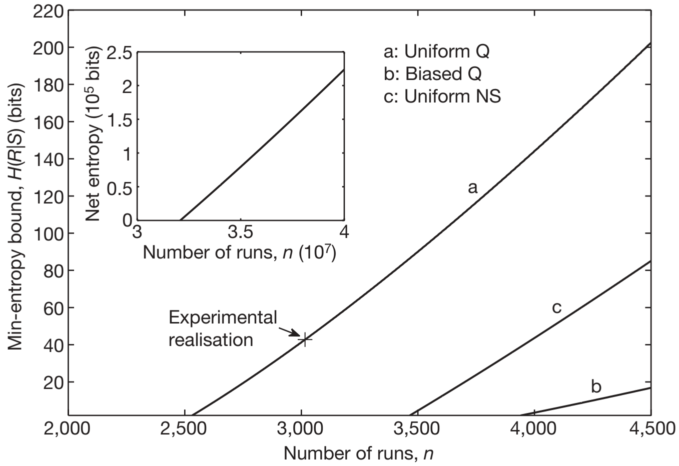

Figure 3 | Bound *nf*(*I*) on the minimum entropy produced versus the number of trials *n* for an observed CHSH violation of $\hat{I} = 2.414$, and a confidence level $1 - \delta = 99\%$. The amount of randomness given by the bound (equation (3)) depends on the probability with which the inputs of each trial (x_i, y_i) are chosen through the parameter $q = \min_{x,y}[P(x, y)]$, where $P(x, y)$ is the probability distribution of the inputs. We have plotted the bounds on the entropy implied by quantum theory for a uniform choice of inputs $[P(x, y) = 1/4]$ (curve a) and for a biased choice of inputs given by $P(00) = 1 - 3q$, $P(01) = P(10) = P(11) = q$, where $q = \alpha n^{-1/2}$ with $\alpha = 11$ (curve b). For a given number n of uses of the devices, the uniform choice of inputs leads to more randomness in the outputs. On the other hand, biased inputs require less randomness to be generated, and the net amount of randomness produced (given by the difference between the output and input entropy) becomes positive for sufficiently large n. Curve c represents the bound on the entropy implied by the no-signalling principle alone for a uniform choice of inputs. Note that in all cases, a minimal number of uses of the devices (a few thousand) is required to guarantee that some randomness has been produced at the confidence level $1 - \delta = 99\%$ The inset shows the net amount of entropy produced (output entropy minus input entropy) for the biased choice of inputs with the observed CHSH violation.

the information of an adversary. The bound, equation (3), establishes security of our randomness expansion protocol against an adversary that measures his side-information before the randomness extraction step; for example, against an adversary that has only a short-lived or bounded quantum memory. This is because it applies when conditioned to any measurement performed by the adversary. However, our protocol is not yet proven to be universally composable against a full quantum adversary, that is, secure against an adversary that stores his side-information in a quantum memory which can be measured at a later stage. A universally composable proof would also cover the situation in which the adversary tries to estimate the random numbers after getting partial information about them. Proving universally composable security of our protocol would also probably lead to much more efficient randomness expansion schemes. Note that the fact that the bound, equation (3), holds for devices that have an internal memory is a significant advance over the device-independent protocols[9,12,13] proposed so far. It is the crucial feature that makes our protocol practical.

The experimental realization of this scheme requires the observation of a Bell inequality with the detection loophole closed (near-perfect detection of every event), so that the outputs r cannot be deterministically reproduced. The two individual systems should also be sufficiently separated so that they do not interact, but it is not necessary for the two subsystems to be space-like separated (Supplementary Information C).

We realize this situation with two $^{171}\mathrm{Yb}^+$ atomic ion quantum bits (qubits)[25] confined in two independent vacuum chambers separated by about 1 m. The qubit levels within each atom are entangled through a probabilistic process whereby each atom is entangled with emitted photons and the interference and coincident detection of the two photons heralds successful preparation of a near-maximal entangled state of the two remote atomic qubits through entanglement swapping[26], as described in Fig. 1 and Supplementary Information D. The binary values a and b correspond to subsequent measurement results of each qubit obtained through standard atomic fluorescence techniques (detection error $<3\%$)[25], and every event is recorded. The respective binary measurement bases x and y are chosen randomly and set by coherent qubit rotation operations before measurement. Direct interaction between the atoms is negligible and classical microwave and optical fields used to perform rotations and measurements on one atom have no influence on the other atom (we perform statistical tests to verify that the measurement data are compatible with this hypothesis; Supplementary Information D.4). To estimate the value of the CHSH inequality, we accumulate $n = 3{,}016$ successive entanglement events over the period of about one month, summarized in Supplementary Information D.1 and Table 1. The observed CHSH violation of $\hat{I} = 2.414$ represents a substantial improvement over previous results[26,27]. The probability that a local theory, possibly including an internal memory of past events[28], could produce such a violation is $P(\hat{I} \geq 2.414) \leq 0.00077$ (Supplementary Information D.3).

In the experiment, we chose a uniform random distribution of the initial input measurement bases, $P(x, y) = 1/4$, to minimize the number of runs required to obtain a meaningful bound on the output entropy (Fig. 3). The observed CHSH violation implies that at least $H(R|S) > 42$ new random bits are generated in the experiment with a 99% confidence level. This is the first time that one can certify that new randomness is produced in an experiment without a detailed model of the devices. We rely only on a high-level description (atoms confined to independent vacuum chambers separated by one metre) to ensure the absence of interaction between the two subsystems when the measurements are performed. As no active measures are taken in our experiment to control this interaction, these new random bits cannot be considered private in the strongest adversarial device-independent scenario. The level of security provided by our experiment will nevertheless be sufficient for many applications, as it guarantees that almost all failure modes of the devices will be detected. The current experiment does not reach the catalysis regime mentioned above, owing to the low success probability of heralded entanglement generation (2×10^{-8}) (ref. 26). However, it should be possible to exceed the catalysis threshold by improving the photon-collection efficiency through the use of nearby optical collection elements or optical cavities[29].

Stepping back to the more conceptual level, we note that equation (3) relates the random character of quantum theory to the violation of Bell inequalities. This bound can be modified for a situation where we assume only the no-signalling principle instead of the entire quantum formalism (Figs 2 and 3 and Supplementary Information A.3). Such a bound lays the basis for addressing in a statistically significant way one of the most fundamental questions raised by quantum theory: whether our world is compatible with determinism (but then necessarily allows signalling between space-like separated

Table 1 | Experimental results

Inputs (x, y)	Rotations (φ_x, φ_y)	$N(0, 0; x, y)$	$N(0, 1; x, y)$	$N(1, 0; x, y)$	$N(1, 1; x, y)$	Total events	$P(a = b \mid xy)$
0, 0	0°, 45°	293	94	70	295	752	0.782
0, 1	0°, 135°	298	70	74	309	751	0.808
1, 0	90°, 45°	283	69	64	291	707	0.812
1, 1	90°, 135°	68	340	309	89	806	0.195

Observed number of events $N(a, b; x, y)$ for which the measurement on one atom gave outcome a and the measurement on the other atom gave outcome b, given the binary choices of the measurement bases (x, y) corresponding to $\pi/2$ qubit rotations with phase angles (φ_x, φ_y) on the equator of the Bloch sphere. The last column gives the fraction of events where $a = b$ given each input. If the experiment is interpreted as consisting of identical and independent realizations (an assumption not made elsewhere in this paper), the data then indicate a CHSH observable of $\hat{I} = \sum_{x,y} (-1)^{xy} [P(a = b|xy) - P(a \neq b|xy)] = 2.414 \pm 0.058$, significantly beyond the local-deterministic threshold of $I = 2$.

regions), or is inherently random (if signalling between space-liked separated regions is deemed impossible).

Received 25 November 2009; accepted 18 February 2010.

1. Knuth, D. *The Art of Computer Programming* Vol. 2, *Seminumerical Algorithms* (Addison-Wesley, 1981).
2. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71,** 1675–1680 (2000).
3. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47,** 595–598 (2000).
4. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93,** 031109 (2008).
5. Atsushi, U. *et al.* Fast physical random bit generation with chaotic semiconductor lasers. *Nature Photon.* **2,** 728–732 (2008).
6. Fiorentino, M., Santori, C., Spillane, S. M., Beausoleil, R. G. & Munro, W. J. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75,** 032334 (2007).
7. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
8. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
9. Masanes, L. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.* **102,** 140501 (2009).
10. Mayers, D. & Yao, A. in *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science* 503–509 (IEEE Computer Society, Washington DC, 1998).
11. Magniez, F., Mayers, D., Mosca, M. & Ollivier, H. in *Proceedings of ICALP 2006* Part I (eds Bugliesi, M. *et al.*) 72–83 (Lecture Notes in Computer Science 4051, Springer, 2006).
12. Acin, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
13. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *N. J. Phys.* **11,** 045021 (2009).
14. Colbeck, R. *Quantum and Relativistic Protocols for Secure Multi-Party Computation.* PhD dissertation, Univ. Cambridge (2007).
15. Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* (Cambridge Univ. Press, 2004).
16. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness. Available at ⟨http://www.stat.fsu.edu/pub/diehard/⟩ (2008).
17. Rukhin, A. *et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (Special Publication 800–22 Revision 1, National Institute of Standards and Technology, 2008); available at ⟨http://csrc.nist.gov/publications/PubsSPs.html⟩.
18. Matsumoto, M. & Nishimura, T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.* **8,** 3–30 (1998).
19. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880–884 (1969).
20. Fine, A. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.* **48,** 291–295 (1982).
21. Koenig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55,** 4337–4347 (2009).
22. Navascues, M., Pironio, S. & Acin, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *N. J. Phys.* **10,** 073013 (2008).
23. Navascues, M., Pironio, S. & Acin, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98,** 010401 (2007).
24. Nisan, N. & Ta-Shma, A. Extracting randomness: a survey and new constructions. *J. Comput. Syst. Sci.* **58,** 148–173 (1999).
25. Olmschenk, S. *et al.* Manipulation and detection of a trapped Yb^+ hyperfine qubit. *Phys. Rev. A* **76,** 052314 (2007).
26. Matsukevich, D. N., Maunz, P., Moehring, D. L., Olmschenk, S. & Monroe, C. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.* **100,** 150404 (2008).
27. Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409,** 791–794 (2001).
28. Gill, R. D. in *Mathematical Modelling in Physics, Engineering and Cognitive Sciences* Vol. 5, *Proceedings of the International Conference on Foundations of Probability and Physics – 2* (ed. Khrennikov, A.) 179–206 (Växjö Univ. Press., Växjö, 2003).
29. Luo, L. *et al.* Protocols and techniques for a scalable atom-photon quantum network. *Fortschr. Phys.* **57,** 1133–1152 (2009).

Supplementary Information is linked to the online version of the paper at www.nature.com/nature.

Acknowledgements We thank R. Colbeck for sharing his PhD thesis with us. This work was supported by the Swiss NCCR Quantum Photonics, the European ERC-AG QORE, the European projects QAP and COM-PAS, the ERC starting grant PERCENT, the Spanish MEC FIS2007-60182 and Consolider-Ingenio QOIT projects, Generalitat de Catalunya, Caixa Manresa, Fundacio Cellex Barcelona, the Interuniversity Attraction Poles Photonics@be Programme (Belgian Science Policy), the Brussels-Capital Region through the project CRYPTASC and a BB2B Grant, the US Army Research Office with funds from IARPA, the National Science Foundation (NSF) Physics at the Information Frontier Program, and the NSF Physics Frontier Center at JQI.

Author Contributions S.P., A.A., S.M. and A.B.d.I.G. developed the theoretical aspects of this work. D.N.M., P.M., S.O., D.H., L.L., T.A.M. and C.M. performed the experiments.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Correspondence and requests for materials should be addressed to A.A. (antonio.acin@icfo.es).